Hogyan mérhető a számítógépes biztonságra fordított pénz?

A különféle IT-beruházások tervezése során időről időre felmerül a kérdés, hogy miként mérhető a biztonsági eszközökre fordított összegek megtérülése, illetve mikor tekinthető hatékonynak egy-egy biztonsági projekt. A NetIQ szakértői szerint a sikeresség pontos meghatározására, illetve az üzleti és a biztonsági célok összehangolására kell helyezni a hangsúlyt.

A biztonsági szoftverek maguk is óriási mennyiségű adatot képesek közölni a működésük eredményességéről: kimutatják, hogy a segítségükkel hány támadást hárítottunk el, hány rendszert tudtunk megerősíteni, vagy éppen mennyire felelnek meg a házirendek és biztonsági előírások a compliance feltételeknek. Egyszerűnek tűnik ezekre a mindig kéznél lévő adatokra hagyatkozni, de hogyan tudjuk közülük kiválasztani, hogy melyik mérőszám igazolja a biztonsági megoldások eredményességét a teljes vállalat üzleti célkitűzéseinek tükrében?

A hosszú ideje működő, érett szervezeteknél gyakori, hogy a kockázatokra és azok kezelésére fókuszálnak, ami érthető is, hiszen tulajdonképpen ez az IT-biztonság alapja. Ugyanakkor még a legprofibb vállalatok is beleesnek néha abba a csapdába, hogy rossz kritériumok alapján értékelik a tevékenységüket. Ahhoz, hogy a biztonsági programok valós eredményeit mérhessük, meg kell határoznunk, mit is jelent a sikeresség az adott területen.

A biztonsági csapatok, minden más részleghez hasonlóan általában szeretik maguk meghatározni, mi alapján mérjék az eredményességet. Amikor azonban a költségvetés jóváhagyásáról, illetve általános üzleti célkitűzések teljesítéséről van szó, nem kizárólag a cégen belüli érdekeltek döntenek az egyes faktorokról. Ezeknek a tényezőknek az üzleti igényeknek megfelelően kell alakulniuk. A legtöbb esetben problémát jelent, hogy a vállalatnál általában nem tudják annál pontosabban leírni, mit várnak a biztonsági részlegtől, mint „ne hackeljenek meg minket” és „legyenek elégedettek az auditorok”.

A biztonsági csapatok és az üzleti vezetők közötti szakadék viszonylag egyszerűen áthidalható, ha közösen használják a GOSPA tervezési eszközt. A rövidítés a Goals, Objectives, Strategies, Plans és Actions szavakat takarja, és a következő, egymásra épülő szakaszokra bontja le a folyamatot: (nagyobb) célkitűzések, (kisebb) célok, stratégiák, tervek és konkrét lépések.

Kezdésként érdemes egy vagy több átfogóbb, realisztikus célkitűzést meghatározni, például: minimalizáljuk az adatszivárgás vagy az adatvesztés kockázatát! Ennek megvalósításához hozzárendelhetünk célokat, például: csökkentsük a rendszerfrissítések telepítésére fordított időt 50 százalékkal, terjesszük ki a kétfaktoros autentikációt megkövetelő hozzáférést az érzékeny adatok 100 százalékára, illetve felügyeljük minden rendszergazda tevékenységét! Az egyes célok megvalósításához ezután készíthetünk stratégiákat, ezeket pedig lebonthatjuk tervekre, illetve feladatokra, amelyek alapján már az egyes területekért felelős szakemberek pontosan a célkitűzésekkel összhangban végezhetik el a munkát.

A stratégia és az egyes lépések gondoskodnak a sikeres működésről az általános üzleti területeken, a mérhető komponenseknek azonban a célok számítanak, ezeket kell tehát a biztonsági és üzleti vezetőknek együttesen meghatározniuk. Ebben a folyamatban fontos szerepet játszik a költségek ismertetése. Ha az üzleti döntéshozók sokallják az

összegeket, akkor át lehet alakítani a célokat az alacsonyabb költségekhez igazítva.

A biztonsági és üzleti vezetők között kétirányú kommunikációra van szükség. Egyrészről fontos, hogy a biztonsági részleg tájékoztassa a döntéshozókat arról, mire van szükség a célkitűzések eléréséhez. A másik oldalon viszont az is elengedhetetlen, hogy az üzleti vezetők pontosan ismertessék a terveket és prioritásokat, azaz bemutassák a saját sikereikhez kapcsolódó mérőszámokat. Az aktuálisan betervezett projekteket legalább évente érdemes felülvizsgálni olyan szempontból is, hogy még mindig szükségesek-e, illetve összhangban állnak-e az aktuális üzleti célokkal.

Példaként említve nem megfelelőek a biztonsági részleg céljai, ha a teljes éves költségvetést a legújabb generációs tűzfalakra fordítják, miközben a legfontosabb üzleti cél egy, az ügyfelekkel szorosabb kapcsolatot biztosító mobil alkalmazás bevezetése az aktuális pénzügyi évben. Hiszen ilyen esetben az az elsődleges, hogy a vásárlók adatainak biztonságáról gondoskodjunk, és megakadályozzunk bármilyen adatlopást vagy -szivárgást az applikáción keresztül. A gyorsuló digitális átalakulás mellett pedig létfontosságú észben tartani, hogy egyre rövidebb idő alatt kell módosítani a biztonsági intézkedéseken, mivel a vállalatoknak lépést kell tartaniuk a versenytársaikkal a folyamatosan változó üzleti igények kielégítésében.

Forrás: https://sg.hu/cikkek/it-tech/127021/hogyan-merheto-a-szamitogepes-biztonsagra-forditott-penz

Válogatta: Berke Barnabásné